

IPCS Group

Contending with Today's Leading Data Threats
in Electronic and Mobile Commerce



CryptoPhone 220 - Voice encryption and integration of SafeGuard PDA in the firmware

- **Secures your voice privacy**
- **Strongest and most secure algorithm available today**
– AES 256 and Twofish
- **4096bit Diffie-Hellman key exchange with SHA256 hash function**

Interoperability

Fully compatible with all CryptoPhone cellular, satellite and fixed-line products, works in any 900/1800/1900 GSM network that provides data call facilities;

Dimensions & Weight

108 x 56 x 18 mm, 160 g, incl. battery, integrated antenna;

Operational Features

Talk time up to 3.5 hours, standby time 180 hours;

Standard Accessories

100-240V AC adapter, USB sync cable, stereo headset with microphone (2.5 mm plug)

First Security Solution for Speech and Data Encryption on PDAs

"Recent events have shown just how seriously organizations take the protection of their company data and telephone calls within a global competitive environment. In order to equip companies and authorities with the technological means to protect themselves against unauthorized data access and phone tapping on smart phones, we have joined forces with Utimaco and GSMK, both from Germany. Together, we offer the first security solution capable of fulfilling these growing security demands," says Dr. Igor Lyszkiewicz of IPCS Group.

GSML is the technological leader in mobile voice encryption, Utimaco is the technological leader in mobile data security. Together they are the perfect partner for us to be able to offer our corporate and government customers not only data and access security but also tap proofing for their mobile devices."

Trustworthy Voice Encryption

The CryptoPhone 220 comes with full source code available for independent assessment to ensure that you can rely on strong encryption without any backdoors in the communications device that you entrust your security to. The CryptoPhone 220 enables you to put the trust where it belongs – in a trustworthy, open and scientific verification process.

CryptoPhone 220 technology is based on well-researched algorithms for both encryption and voice processing. It features the strongest encryption available combined with key lengths that provide peace of mind today and in the future.

CryptoPhone 220 Overview

Generic GSM Services

Call holding, waiting, forwarding, barring, Calling Line Identification (CLI), SMS, network selection, cell broadcast.

Connectivity

Mini-USB connector (Slave USB, Power in), SDIO/MMC memory card slot, Bluetooth V 1.1

Supported Profiles – Generic Access Profile, Serial Port Profile, headset profile, Generic Object Exchange Profile, Hands-free Profile;

Display

Sunlight-readable 2.8" TFT LCD screen with LED backlight, 40 x 350 pixels, 64K colors;

Keyboard / Buttons

2.8" touch screen, talk / hang-up buttons, 5-way navigation keypad plus dedicated contacts, calendar, voice recorder and camera capture buttons, volume up / down buttons.

Audio

Audio codecs – Encrypted calls – CELP, voice recorder (not encrypted), AMR, decoding/playback, WAV/WMA/AMR/AAC/MP3, polyphonic ring tones;

CMOS Camera

With 1.3 megapixels resolution and preview mirror (can be completely disabled upon request);

Notification

Green/red/blue LEDs for GSM network status, power change status, PDA notification, Bluetooth connectivity status, customizable vibration alert for notification and incoming calls;;

Optional Accessories

Spare batteries, 12V cigarette lighter charger, solar panel charger, vehicle mount kit, noise-cancellation headset, ruggedized military carrying case;

Satellite Upgrade Option

Upgradeable to dual-mode secure GSM and Thuraya satellite communications.

IPCS Group

IPCS Ltd.

• 13/F, Silver Fortune Plaza
1 Wellington Street, Central, Hong Kong
Tel: (852) 2525 7718 Fax: (852) 2140 6833

IPCryptSIM Inc.

• Unit 12C, 12/F, Goldland Tower, 10, Eisenhower St.,
Greenhills, San Juan, 1503 Metro Manila, Philippines
Tel: (63 2) 3961061 Fax: (63 2) 6473499

BICS Sdn. Bhd.

• 8.01, Level 8, AMODA Building,
22, Jalan Imbi, 55100 Kuala Lumpur, Malaysia
Tel.: 60 3 2144 7000 Fax.: 60 3 2144 8959



SafeGuard PDA Data Security

Security

- Secure user authentication
 - Alternatively via password, symbol or numeric PIN,
 - x.509 certificate-logout
 - Organization specific password rules
 - Increasing delay time with increasing number of false tries
 - Alarm sound or complete memory erase in case a definable threshold of false tries is exceeded*)
- Secure Screen Saver
- Device lockdown functions securing the configuration
 - Optional central blocking of infrared port, Bluetooth, WLAN, 'autorun' and memory card

Comprehensive encryption capabilities

- PIM databases (calendar, contacts, tasks, E-mails/SMS)
 - fully transparent at run-time on Windows Mobile
- Files in local RAM, flash file store
- All current storage card formats
- GSM voice encryption without additional hardware components via GSMK CryptoPhoneTM
- Encryption compatible to SafeGuard PrivateDisk and SafeGuard PrivateCrypto, exchange of encrypted data between PDA and PC via E-Mail or memory card*)

System administration

- Central configuration via Microsoft Management Console (MMC) or reference device (Palm OS)
- Configurable user appearance, security settings, encryption and password rules
- Administration rights for end users, collectively or individually configurable by system administrator
- Central distribution of security settings via:
 - Dedicated third party software management tools (e.g. Extended Systems Onebridge, Sybase Pylon)
- Protection against unauthorized de-installation
- Optional automated re-activation after a hard reset including the recently valid settings and passwords for continuous protection of the PDA rendering it useless to a thief (on Windows Mobile 2003 and Palm OS PDAs with persistent Flash Filestore and 'autorun' capability)

Ease of use

- Automated encryption without user intervention
- Efficient algorithms – negligible performance impact
- Secure and powerful challenge/response procedure to reset forgotten passwords without the need for on-line connection

Certifications

- Designed for Windows Mobile 2003
- Symbian Signed
- FIPS 140-2 for SafeGuard PDA (cryptographic library in evaluation)

Complementary SafeGuard® products

- SafeGuard PrivateDisk for exchanging virtual encrypted volumes on storage cards with PC platform*)
- SafeGuard PrivateCrypto for exchanging encrypted E-mail attachments or files with PC platform*)
- SafeGuard Easy for protecting data stored on PC clients via harddisk encryption and pre-boot authentication
- SafeGuard Web Helpdesk, Web Selfhelp or CryptoServer

Helpdesk – alternatives to recover from forgotten passwords Interoperability

- SafeGuard PDA is compatible with all leading software distribution tools for PDAs
- VOICE.TRUST server for automated biometric challenge/response helpdesk

Standards/Protocols

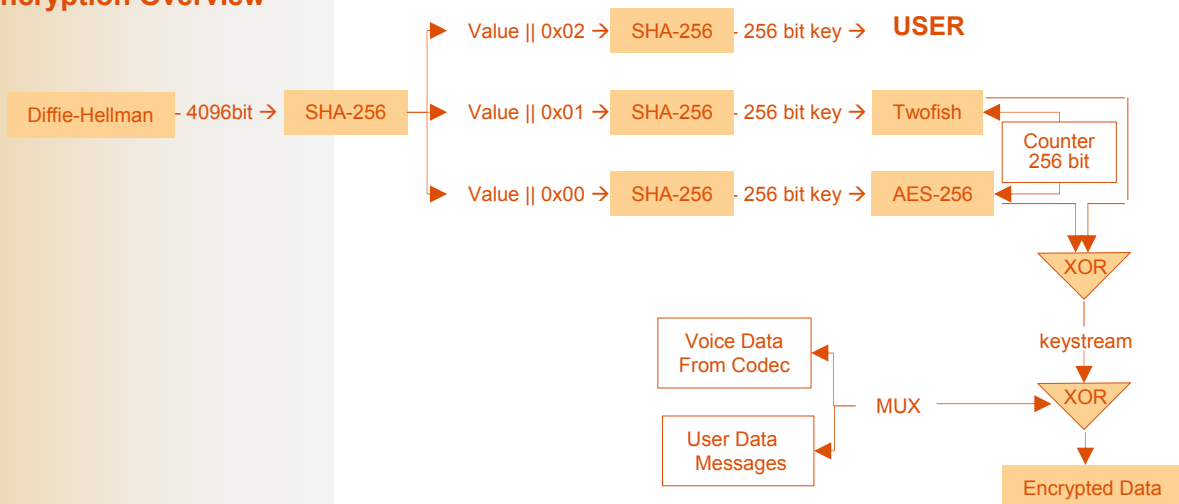
- AES (128 and 256 bit), PKCS#5

Language Versions

- English, German, French, Japanese

[Specifications may change with newer versions]

Voice Encryption Overview



Find out how to protect yourself.

Look how easy it is!